Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2010, Article ID 782438, 11 pages
doi:10.1155/2010/782438

Research Article

On Converting Secret Sharing Scheme to Visual Secret Sharing Scheme

Daoshun Wang and Feng Yi

Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Correspondence should be addressed to Daoshun Wang, wangdaoshun@gmail.com

Received 25 November 2009; Revised 28 April 2010; Accepted 4 July 2010

Academic Editor: Yingzi Du

Traditional Secret Sharing (SS) schemes reconstruct secret exactly the same as the original one but involve complex computation. Visual Secret Sharing (VSS) schemes decode the secret without computation, but each share is m times as big as the original and the quality of the reconstructed secret image is reduced. Probabilistic visual secret sharing (Prob.VSS) schemes for a binary image use only one subpixel to share the secret image; however the probability of white pixels in a white area is higher than that in a black area in the reconstructed secret image. SS schemes, VSS schemes, and Prob. VSS schemes have various construction methods and advantages. This paper first presents an approach to convert (transform) a (k, k)-SS scheme to a (k, k)-VSS scheme for greyscale images. The generation of the shadow images (shares) is based on Boolean XOR operation. The secret image can be reconstructed directly by performing Boolean OR operation, as in most conventional VSS schemes. Its pixel expansion is significantly smaller than that of VSS schemes. The quality of the reconstructed images, measured by average contrast, is the same as VSS schemes. Then a novel matrix-concatenation approach is used to extend the greyscale (k, k)-SS scheme to a more general case of greyscale (k, n)-VSS scheme.

1. Introduction

A secret kept in a single information-carrier could be easily lost or damaged. Secret Sharing (SS) schemes, called (k, n) threshold schemes, have been proposed since the late 1970s to encode a secret into n pieces ("shadows" or "shares") so that the pieces can be distributed to n participants at different locations [1, 2]. The secret can only be reconstructed from k or more pieces ($k \leq n$). Since Shamir's scheme is a basic secret sharing scheme and is easy to implement, it is commonly used in many applications. However, the computation complexity of Shamir's scheme is $O(k \log^2 k)$ for the polynomial evaluation and interpolation in [3]. Wang et al. [4] proposed a deterministic (k, k)-secret sharing scheme for greyscale images. That scheme uses simple Boolean XOR operations and has no pixel expansion. The computation complexity of the reconstructed secret image is $O(k)$. Visual secret sharing (VSS) schemes [5] have been proposed to encode a secret image into n "shadow" ("share") images to be distributed to n participants. The secret can be visually reconstructed only when k or more shares are available. No information will be revealed with any $k - 1$ or fewer shares. VSS schemes, originally based on binary images, have been expanded to work with greyscale and color images. In a (k, n)-VSS scheme, the computation complexity of reconstructing a secret image using k shadows in visual cryptography is proportional to $O(k)$ and proportional to the size of the shadow images. Several (k, k)-VSS schemes have been designed for special k values [6–8]. In a VSS scheme, every pixel of the original image is expanded to m subpixels in a shadow image. These m subpixels are referred to as pixel expansion. The quality of the reconstructed secret image is evaluated by contrast (denoted by α) in VSS schemes. Pixel expansion m and contrast α are two factors to evaluate a VSS scheme. Therefore, it is desirable to minimize m and maximize α as much as possible. Much work has been directed toward reducing the pixel expansion [9, 10]. Many of the previous schemes were primarily proposed for binary images. A number of VSS schemes have also been proposed for greyscale images [11–13]. The minimum pixel expansion of the (k, k)-VSS scheme for greyscale image in [13] is equal to those in [11, 12], namely, $m \geq (g - 1) \cdot 2^{k-1}$, where g is the number of different grey levels in the secret image. The deterministic VSS schemes mentioned above have achieved minimum pixel expansion m and optimal contrast $\alpha = 1/m$, but the value of m can be still quite large, partly because m is proportional to the exponential of k.

To further reduce pixel expansion, a number of probabilistic VSS schemes (Prob.VSS schemes) have been proposed in [14–16]. These schemes were designed for the case of $g = 2$, that is, for black and white images. In the reconstructed secret image, the probability of white pixels in a white area is higher than that in a black area. Therefore small areas, rather than individual pixels, of the secret image can be recovered accurately. With the trade-off in resolution, probabilistic schemes can achieve no pixel expansion ($m = 1$), and the contrast is the same as the ones in the deterministic schemes.

Because the SS scheme, VSS scheme, and Prob. VSS scheme use these different construction methods, it is important to research the link (or relationship) among these three methods. Some studies have focused on describing the relationship of SS schemes and VSS schemes with respect to pixel expansion and contrast. Cimato et al. [16] first proved that there exists a one-to-one mapping between binary VSS schemes and probabilistic binary VSS schemes with no pixel expansion, where contrast is traded for the probability factor. Yang et al. [17, 18] introduced secret image sharing deterministic and probabilistic visual cryptograph scheme (DPVCS), which is a two-in-one combination of VSS and PVSS schemes. Bonis and Santis [19] first analyzed the relationship between SS schemes and VSS schemes, focusing attention on the amount of randomness required to generate the shares. They proved that SS schemes for a set of secrets of size two binary SS schemes and VSS schemes are "equivalent" with respect to the randomness. Lin et al. [20] presented an innovative approach to combine two VSS and SS scheme, the n shares are created for a given grey-valued secret image. Each share includes both SS and VSS scheme information, providing two options for decoding. So far the study of relationships among SS, Prob. VSS, and VSS scheme has been focused mainly on the relationship between VSS and Prob. VSS scheme, the randomness relationship between SS and VSS scheme, and the methods combining VSS and SS scheme. However, another interesting topic of study would be the relationship between SS and VSS schemes, especially with regard to the underlying pixel expansion and contrast.

In this paper, we give the relationship between the (k, n)-SS scheme and (k, n)-VSS scheme with respect to pixel expansion and contrast. We first propose a construction approach to transform a traditional (k, k)-SS scheme to a (k, k)-VSS scheme for greyscale images. That is, the generation of the shadow images is based on Boolean OR and XOR operations, and the reconstruction process uses Boolean OR operation, as in most other VSS schemes. In our (k, k)-VSS scheme, the pixel expansion m is $g - 1$, much smaller than the $(g - 1) \cdot 2^{k-1}$ of traditional VSS scheme and independent of k. The quality of the reconstructed image, measured in "Average Contrast" between consecutive grey levels, is $1/(g - 1) \cdot 2^{k-1}$, which is equal to that in the VSS schemes. Then we extend the traditional (k, k)-SS scheme to a (k, k)-VSS scheme for greyscale images. In our (k, n)-scheme, the pixel expansion is smaller than that of previous deterministic (k, n)-VSS schemes [10, 11], when $k \geq n/4$, $k \geq 4$. The average contrast of our (k, n)-VSS scheme is close to that of deterministic (k, n)-VSS schemes [10, 11] when $k \geq n/2$, $k \geq 2$.

The rest of the paper is organized as follows. In Section 2, we briefly review binary Prob. VSS scheme. Section 3 presents an approach to convert a greyscale (k, k)-SS scheme to a (k, k)-VSS scheme. In Section 4, we present a novel approach to extend the above (k, k)-SS scheme into a more general greyscale (k, n)-VSS scheme. Section 5 concludes the paper.

2. A Review of Probabilistic VSS Scheme

Here, we briefly review probabilistic visual secret sharing scheme [14–16]. The following Definition 2.1 is directly from Yang's scheme [15].

Definition 2.1 (see [15]). A (k, n)-Prob. VSS scheme can be shown as tow sets, white set C_0 and black set C_1, consisting of n_λ and n_γ $n \times 1$ matrices, respectively. When sharing a white (resp., black) pixel, the dealer first randomly chooses one $n \times 1$ column matrix in C_0 (resp., C_1), and then randomly selects one row of this column matrix to a relative shadow. The chosen matrix defines the color level of pixel in every one of the n shadows. A Prob. VSS Scheme is considered valid if the following conditions are met.

(1) For these n_λ (resp., n_γ) matrices in the set C_0 (resp., C_1) the "OR"-ed value of any k-tuple column vector V is $L(V)$. There values of all matrices form a set λ (reps. γ).

(2) The two sets λ and γ satisfy that $p_0 \geq p_{\mathrm{TH}}$ and $p_1 \leq p_{\mathrm{TH}} - \alpha$, where p_0 and p_1 are the appearance probabilities of the "0" (white color) in the set λ and γ, respectively.

(3) For any subset with $\{i_1, i_2, \ldots, i_q\}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the p_0 and p_1 are the same.

The first two conditions are called contrast, and the third is condition called security. From the above definition, the matrices in C_0 and C_1 are $n \times 1$ matrices, so the pixel expansion is one.

For conventional VSS schemes, a pixel in the original image is expanded to m subpixels and the number of white subpixels of a white and black pixel is h and l. When stacking k shadows, we will have "$m - h$" B "h" W subpixels for a white pixel and "$m - l$" B "l" W subpixels for a black pixel. Hence, from the observation, if we use all the columns of the basis matrices S^0 and S^1 of a conventional VSS scheme as the $n \times 1$ column matrices in the sets C_0 and C_1, we can let the pixel appear in white color different probability instead of expanding the original pixel to m subpixel and the frequency of white pixel in white and black areas in the recovered image will be $p_0 = h/m$ and $p_1 = l/m$.

3. The Proposed Converting Method for a (k, k) Scheme

The purpose of this section is to show how to convert a (k, k)-SS scheme to a (k, k)-VSS scheme. First, we give quality measures of the recovered secret image. Then we introduce a seemingly simple but very valid method that can be used easily to transform a greyscale image to a binary image. Finally, we prove that the proposed method for converting the (k, k)-SS scheme to a (k, k)-VSS scheme is valid.

3.1. Quality Measurement of Recovered Secret Image. Since the existing probabilistic schemes were only proposed for binary images, the contrast between black and white pixels was naturally chosen as an important measurement of quality. The scheme we proposed is for greyscale images. We use the expected contrast between two pixels with consecutive grey levels in the original image to indicate the quality of reconstruction. This is referred to as "Average Contrast", defined as follows.

Let $S = [s_{ij}]$ be the $\phi \times \varphi$ original secret image, $i = 1, 2, \ldots, \phi$, $j = 1, 2, \ldots, \varphi$, and $s_{ij} \in \{1, \ldots, g\}$. Suppose that $U = [u_{ij}]$ is the $(m_g \cdot \phi) \times (m_g \cdot \varphi)$ reconstructed image, where m_g is the pixel expansion factor. For $s_{ij} = l$, $l \in \{1, \ldots, g\}$, the corresponding pixel in Ucan be denoted as $U_l = \{u_{ij} \mid s_{ij} = l\}$, $l \in \{1, \ldots, g\}$.

The appearance of U_l depends on the Hamming weight of the m dimensional vector. Because of the randomness of the shadow images, $H(U)$ is a random variable. We are interested in the average Hamming weight for all pixels U_l.

Let $a_{ij}^{(h)}$ be the (i, j)th Boolean value in the hth shadow image. Then the reconstruction results is

$$u_{ij} = a_{ij}^{(1)} + a_{ij}^{(2)} + \cdots + a_{ij}^{(k)}. \tag{1}$$

The symbol "+" represents Boolean OR operation in formula (1). In other words, matrix U is Boolean OR operation of the shares $U = A_1 + \cdots + A_k$.

Let $P_t = \mathrm{P}(H(\{u_{ij} = t \mid s_{ij} = l\}))$ be the probability of $H(U_l)$ taking value t with $t \in \{1, \ldots, g\}$, the expected value of $H(U_l)$ is $E(H(\{u_{ij} = t \mid s_{ij} = l\})) = \sum_{t=0}^{g-1} t \cdot P_t$. We now define Average Grey β_l and Average Contrast α_l for the reconstructed image as

$$\beta_l = E\left(\frac{H\left(u_{ij} \mid l\right)}{m_g}\right) = \frac{E\left(H\left(\left\{u_{ij} = t \mid s_{ij} = l\right\}\right)\right)}{m_g}, \qquad \alpha_l = \beta_l - \beta_{l-1}, \quad l \in \{2, \ldots, g\}. \tag{2}$$

3.2. Brief Review the (k, k)-SS Scheme Based on Boolean XOR Operation. The (k, k)-SS scheme in [4] is deterministic and the reconstructed image is exactly the same as the original one. A secret image S can share k shadows $A_1, \ldots, A_k$. After obtaining all k shadows, we can perform XOR operations to recover the secret image A.

The (k, k)-SS scheme in [4] for greyscale images is given in Algorithm 1.

From Algorithm 1, the symbol "$\oplus$" represents XOR operation, the computation complexity of reconstructed secret image is $O(k)$. The reconstructed secret image needs to perform Boolean XOR operation described in [15] while conventional VSS scheme performs Boolean OR operation. If a and b are integers, $a \oplus b$ can be expressed in terms of OR and XOR operations as: $a \oplus b = \mathrm{OR}\ (\mathrm{NOT}\ (\mathrm{OR}\ (\mathrm{NOT}\ a, b)),\ \mathrm{NOT}\ (\mathrm{OR}\ (a, \mathrm{NOT}\ b))\ )$. The XOR operation can be performed by four NOT operations and three OR operations. Thus, the scheme described above is more complex than VSS schemes based on OR operations. In this case, we cannot directly use SS scheme of [15] to construct a VSS scheme. A new approach must be constructed. To address this, we propose a method to convert a greyscale secret image to a binary image. Then, we construct a (k, k)-VSS scheme to transform XOR operation to OR operation based on scheme of [15]. The following subsection will introduce this new method to encode greyscale images into binary images.

3.3. New Encoding Method of Greyscale Image. Each pixel of original image S can take any one of g different grey levels. $S = [s_{ij}]_{\phi \times \varphi}$, where $i = 1, 2, \ldots, \phi$, $j = 1, 2, \ldots, \varphi$ and $s_{ij} \in \{1, \ldots, g\}$. We have $g = 2$ for a binary image and $g = 256$ for a greyscale image with one byte per pixel. In a greyscale image with one byte per pixel, the pixel value can be an index to a color table, thus $g = 256$. In a color image using an RGB model, each pixel has three integers: R (red), G (green) and B (blue). If each R, G or B takes value between 0 and 255, we have $g = 256^3$.

In the construction of the shadow images, each pixel of S is coded as a binary string of $g - 1$ bits. For $s_{ij} = l$, its coded form is $c_{ij} = b_{g-1}^{l-1} = 0^{g-l}1^{l-1}$, which is a string of $g - l$ zeros and $l - 1$ ones. The order of the bits does not matter.

Example 3.1. For example, b_{6-1}^{4-1} can be written as 00111, or 01101, or equivalently 11010.

Note that the range of grey level for the original image and the reconstructed image pixels is from 1 to g, but the range of coded form, c_{ij}, is from 0 to $g - 1$. Notation gives a list of variable names for easy lookup.

Each pixel of C is expanded into $g - 1$ subpixels with a function T which converts a binary string of $g - 1$ bits into a row vector of $g - 1$ components. Therefore, the pixel expansion factor of this scheme is $m = g - 1$. Notice that this encoding method turns out to be a crucial part of construction.

3.4. Construction of the Shares. Each pixel of C is expanded into $g - 1$ subpixels with a function T which converts a binary string of $g - 1$ bits into a row vector of $g - 1$ components. Therefore, the pixel expansion factor of this scheme is $m_g = g - 1$.

Now, the description of the proposed scheme is given in Algorithm 2.

3.5. Proof of the Construction. In this section we will show that the quality of the scheme depends on the quality of the reconstructed image U. We now look at a pixel of the

Input: an integer k with $k \geq 2$, and the secret image S.
Output: k distinct matrices $A_1, \ldots, A_k$, called shadow images.
Construction: generate $k-1$ random matrices $B_1, \ldots, B_{k-1}$, compute the shadow images as below:
$A_1 = B_1, \quad A_2 = B_1 \oplus B_2, \ldots, A_{k-1} = B_{k-2} \oplus B_{k-1}, \quad A_k = B_{k-1} \oplus S.$
Revealing: $S = A_1 \oplus A_2 \oplus \cdots \oplus A_k$.

Algorithm 1

Input: The secret image S, $S = [s_{ij}]$ in the coded form $C = [c_{ij}]$
Output: The shadow images $D_1, \ldots, D_k$.
Share generation: Randomly generate $k-1$ matrices $R_1, \ldots, R_{k-1}$ of size $(m_g \cdot \phi) \times (m_g \cdot \varphi)$,
where $R_h = X_h$, $X_h \in \{0, \ldots, 2^{g-1} - 1\}$.

$$D_1 = R_1,$$
$$D_h = R_{h-1} \oplus R_h, \quad h = 2, \ldots, k-1,$$
$$D_k = R_{k-1} \oplus C.$$

The basic construction matrix is $U = \begin{pmatrix} T(D_1) \\ \vdots \\ T(D_k) \end{pmatrix}$, where the transform T converts a binary string of $g-1$ bits into a row vector of $g-1$ components. That is, $T(D_h) = V^{(h)} = (v_1^{(h)} \cdots v_{g-1}^{(h)})$, $h = 1, \ldots, k$. The hth row of the basic matrix is used to construct the share image D_h.
Revealing: $U = D_1 + \cdots + D_k$.

Algorithm 2

reconstructed image $U = D_1 + \cdots + D_k$. Theorem 3.2 states the average grey and average contrast of U.

Theorem 3.2. *The proposed algorithm is a probabilistic* (k, k)*-VSS scheme with Pixel expansion* $m_g = g - 1$, *Average Grey*

$$\beta_l = \frac{E\Big(H\Big(\Big\{u_{ij} = t \mid s_{ij} = l\Big\}\Big)\Big)}{m_g} = \frac{\Big[\Big(1 - 1/2^{k-1}\Big)(g-l) + (l-1)\Big]}{g-1}, \quad l \in \{1, \ldots, g\}, \tag{3}$$

and Average Contrast $\alpha_l = \beta_l - \beta_{l-1} = 1/(2^{k-1} \cdot (g-1))$.

Proof. To show security, since the random matrices $R_1, \ldots, R_{k-1}$ are all distinct, thus the matrices $D_1, \ldots, D_k$ are also all distinct and all random, therefore each share does not reveal any information of S and the security of the scheme is ensured. Then we will prove any $k-1$ or fewer shares will not be obtained any information of C, that is: $D_{i_1} \oplus D_{i_2} \oplus \cdots \oplus D_{i_h} \neq C$ for any set of integers $\{i_1, \ldots, i_h\}$ when $1 \leq h < k$. We consider two cases.

Case 1 ($k \in \{i_1, \ldots, i_h\}$). In this case, $D_k \oplus (\oplus_{j=s}^{t} D_j) = C \oplus R_{k-1} \oplus (\oplus_{j=s}^{t} D_j)$ where $\oplus_{j=s}^{t} D_j$ means $D_s \oplus \cdots \oplus D_t$ with $s, \ldots, t$ being the indices in $i_1, \ldots, i_h$ besides n. Since there are odd number of random matrices involved, at least one of them cannot be absorbed into zero matrix, thus $D_{i_1} \oplus D_{i_2} \oplus \cdots \oplus D_{i_h}$ must be random thus not equal to C.

Case 2 ($k \notin \{i_1, \ldots, i_h\}$). Since no matrix C involved in $D_{i_1} \oplus D_{i_2} \oplus \cdots \oplus D_{i_h}$ to begin with, $D_{i_1} \oplus D_{i_2} \oplus \cdots \oplus D_{i_h}$ is constructed from the random matrices $R_1, \ldots, R_{h-1}$ only and it must be random.

Therefore, the proposed (k, k) scheme satisfies the security condition. That is, when fewer than k shadows are used, the original secret image C will not be revealed.

To show contrast, let m_g be the pixel expansion, we have $m_g = g - 1$ according to the construction of the shares above.

Since $U = T(d_1) + \cdots + T(d_k)$ with "+" being Boolean OR, we have

$$U = T(X_1) + (T(X_1) \oplus T(X_2)) + \cdots (T(X_{k-2}) \oplus T(X_{k-1})) + (T(X_{k-1}) \oplus T(s)). \tag{4}$$

Substituting $T(X_i)$ with V_i, $i = 1, \ldots, k-1$. We use variables V_0 substitute $T(s)$. We get

$$U = V_1 + (V_1 \oplus V_2) + \cdots + (V_{k-2} \oplus V_{k-1}) + (V_{k-1} \oplus V_0), \tag{5}$$

Here, V_0 is the coded from the original image S. That is, $V_0 = 0^{g-l}1^{l-1}$ for $s_{ij} = l$. Since $V_1 + (V_1 \oplus V_2) = V_1 + \overline{V_1} V_2 = V_1 + V_2$ and $V_1 + V_2 + (V_2 \oplus V_3) = V_1 + V_2 + V_3$, we have

$$U_l = \Big\{u_{ij} \mid s_{ij} = l\Big\} = V_1 + V_2 + \cdots + V_{k-2} + V_{k-1} + (V_{k-1} \oplus V_0), \quad l \in \{1, \ldots, g\}. \tag{6}$$

This can be rewritten as

$$U_l = U_0 + V_{k-1} + (V_{k-1} \oplus V_0), \tag{7}$$

where $U_0 = V_1 + V_2 + \cdots + V_{k-2}$.

We know that $V_{k-1} + (V_{k-1} \oplus V_0)$ must have at least $l-1$ bits being 1. That is $V_{k-1} + (V_{k-1} \oplus V_0)$ can be written as $x^{g-l}1^{l-1}$ where each of the $g-l$ bits, denoted by x, may take value 0 or 1. Therefore, $U_l = \{u_{ij} \mid s_{ij} = l\} = U_0 + x^{g-l}1^{l-1} = y^{g-l}1^{l-1}$ also has at least $l-1$ bits being 1. The probability for each y bit to be 1 is $p = 1 - 1/2^{k-1}$ since every of such bit depends on $k-1$ random matrices. The total number of 1's among these $g-l$ bits (the Hamming weight of the vector) is a random variable with a binomial distribution, and the expected value of the Hamming weight is

$$\left(1 - \frac{1}{2^{k-1}}\right) \cdot (g-l) = p(g-l). \tag{8}$$

It follows that the expected Hamming weight of the entire $g-1$ vector is

$$E\left(H\left(\left\{u_{ij} \mid s_{ij} = l\right\}\right)\right) = \left(1 - \frac{1}{2^{k-1}}\right) \cdot (g-l) + (l-1), \quad l \in \{1,\ldots,g\}. \tag{9}$$

Thus the Average Grey is

$$\beta_l = \frac{E\left(H\left(\left\{u_{ij} \mid s_{ij} = l\right\}\right)\right)}{m} = \frac{\left[\left(1-1/2^{k-1}\right)(g-l)+(l-1)\right]}{g-1}. \tag{10}$$

and the Average Contrast of the reconstructed image is

$$\alpha_l = \beta_l - \beta_{l-1} = \frac{1}{2^{k-1} \cdot (g-1)}. \tag{11}$$

□

Example 3.3 (continuation of Example 3.1). According to (9) of Theorem 3.2, we obtain

$$\begin{aligned}
&E\left(H\left(\left\{u_{ij} \mid s_{ij} = 1\right\}\right)\right) \\
&\quad = \left(1 - \frac{1}{2^{k-1}}\right) \cdot (g-l) + (l-1) \\
&\quad = \left(1 - \frac{1}{2^{2-1}}\right) \cdot (3-1) + (1-1) = 1, \\
&E\left(H\left(\left\{u_{ij} \mid s_{ij} = 2\right\}\right)\right) \\
&\quad = \left(1 - \frac{1}{2^{k-1}}\right) \cdot (g-l) + (l-1) \\
&\quad = \left(1 - \frac{1}{2^{2-1}}\right) \cdot (3-2) + (2-1) = \frac{3}{2}, \\
&E\left(H\left(\left\{u_{ij} \mid s_{ij} = 3\right\}\right)\right) \\
&\quad = \left(1 - \frac{1}{2^{k-1}}\right) \cdot (g-l) + (l-1) \\
&\quad = \left(1 - \frac{1}{2^{2-1}}\right) \cdot (3-3) + (3-1) = 2.
\end{aligned} \tag{12}$$

By the definition of Average Grey and Average Contrast (2), $\beta_l = E(H(\{u_{ij} \mid s_{ij} = 1\}))/g-1$, we have Average Grey

$$\begin{aligned}
\beta_1 &= \frac{E\left(H\left(\left\{u_{ij} \mid s_{ij} = 1\right\}\right)\right)}{g-1} = \frac{1}{3-1} = \frac{1}{2}, \\
\beta_2 &= \frac{E\left(H\left(\left\{u_{ij} \mid s_{ij} = 2\right\}\right)\right)}{g-1} = \frac{3/2}{3-1} = \frac{3}{4}, \\
\beta_3 &= \frac{E\left(H\left(\left\{u_{ij} \mid s_{ij} = 3\right\}\right)\right)}{g-1} = \frac{2}{3-1} = 1.
\end{aligned} \tag{13}$$

Average Contrast

$$\alpha_2 = \beta_2 - \beta_1 = \frac{1}{4}, \qquad \alpha_3 = \beta_3 - \beta_2 = \frac{1}{4}. \tag{14}$$

We can reach the exactly same average contrast directly from (11). The average contrast is the same as that of Example 3.3.

The following Theorem 3.4 is directly from the result of [15].

Theorem 3.4 (see [15]). *In binary (k,k)-Prob.VSS scheme with $m = 1$ and the parameters threshold probability $p_{\text{TH}} = 1/2^{k-1}$ and the contrast $\alpha = 1/2^{k-1}$. Suppose that the secret image is black and white image, in our Theorem 3.2 above, Pixel expansion $m_g = g-1$, Average Contrast $\alpha_l = \beta_l - \beta_{l-1} = 1/2^{k-1} \cdot (g-1)$. That is $g = 2$, we obtain $m_2 = 2-1 = 1$, and $\alpha_l = \beta_l - \beta_{l-1} = 1/2^{k-1} \cdot (2-1) = 1/2^{k-1}$. It is clear that values of pixel expansion and contrast of Theorem 3.2 above are same as those of Theorem 3.4.*

3.6. The Minimum Size of Recognizable Regions. With a probabilistic scheme, small regions (not individual pixels) of the secret image are correctly reconstructed. The smaller such regions can be, the better this scheme is. We now discuss the minimum size of the region that can be correctly recognized.

Before examining a region of N pixels, we start with one pixel taking grey level l, that is, $s_{ij} = l$. The reconstructed pixel is $U_l = \{u_{ij} \mid s_{ij} = l\} = x^{g-l}1^{l-1}$, $x \in \{0,1\}$. Let Y_l be the Hamming weight of U, we have $Y_l = H(U_l) \in \{l-1,\ldots,g-1\}$ and

$$P(Y_l = l-1+t) = \binom{g-l}{t} \cdot p^t \cdot (1-p)^{g-l-t}, \tag{15}$$

where $p = 1 - 1/2^{k-1}$. Clearly, Y_l has a binomial distribution with mean and variance being.

We have

$$\mu_y = l-1+p(g-l), \qquad \delta_y^2 = (g-l)p(1-p). \tag{16}$$

Now we consider a group of N pixels with the same grey level l in the original image. Since all pixels are treated separately in the share generation, these N random variables are independent and identically distributed (i.i.d.).

Therefore, the total visual effect of the region is closely related to the $Z = \sum_{i=1}^{N} Y_l^{(i)}$, and

$$\begin{aligned} E(Z) &= E\left(\sum_{i=1}^{N} Y_l^{(i)}\right) = \sum_{i=1}^{N} E\left(Y_l^{(i)}\right) \\ &= N\mu_y = N[p(g-l)+(l-1)], \end{aligned} \tag{17}$$

where $p = 1 - 1/2^{k-1}$,

$$\begin{aligned} \operatorname{Var}(Z) &= \operatorname{Var}\left(\sum_{i=1}^{N} Y_l^{(i)}\right) = \sum_{i=1}^{N} \operatorname{Var}\left(y^{(i)} l\right) = N\sigma_y^2 \\ &= N[p(1-p)(g-l)]. \end{aligned} \tag{18}$$

Based on Central Limit Theory, these binomial distribution can be safely approximated by Gaussian distribution, and we can obtain the lower bound for N. According to Empirical Rule, about 99.73% of all values fall within three standard deviations of the mean. Hence, to recognize a region of grey level l, the region size should satisfy

$$\mu_l - 3\sigma_l > \mu_{l-1} + 3\sigma_{l-1} + N \cdot d, \tag{19}$$

where d determines the minimum separation between the two distributions. That is

$$\begin{aligned} &N[p(g-l)+(l-1)] - 3\sqrt{Np(1-p)(g-l)} \\ &\quad > N[p(g-l+1)+(l-2)] \\ &\quad + 3\sqrt{Np(1-p)(g-l+1)} + Nd, \\ &N[-p+1-d] > 3\sqrt{Np(1-p)(g-l)} \\ &\quad + 3\sqrt{Np(1-p)(g-l+1)}, \\ &N > \frac{3\sqrt{N} \cdot \sqrt{p(1-p)} \cdot \left(\sqrt{(g-l)} + \sqrt{(g-l+1)}\right)}{1-p-d}. \end{aligned} \tag{20}$$

Therefore

$$N > 9p(1-p) \cdot \left(\frac{\sqrt{g-l} + \sqrt{g-l+1}}{1-p-d}\right)^2. \tag{21}$$

Note that the range of original image pixel value is slightly different from the range of its coded form, that is $s_{ij} \in \{1, 2, \ldots, g\}$ and $c_{ij} \in \{0, 1, \ldots, g-1\}$. When $l = g$, the above inequality becomes

$$N > \frac{9p(1-p)}{(1-p-d)^2}, \tag{22}$$

which indicates the minimum size of a recognizable region between grey level g and grey level $g-1$. When $g = 2$, the above is the minimum region size in a binary image. In the (k, n) probabilistic VSS scheme proposed in [15], the minimum region size is

$$N_{\text{Yang}} > 9 \cdot \left(\frac{\sqrt{p_0(1-p_0)} + \sqrt{p_1(1-p_1)}}{p_0 - p_1 - d}\right)^2. \tag{23}$$

Table 1: Minimum region sizes of a binary image with the proposed greyscale (k, k)-VSS scheme or the scheme of [14].

D	Black and white (2, 2)	Black and white (3, 3)
0.00	9	27
0.05	12	43
0.10	15	75
0.15	19	169
0.20	25	675
0.25	36	
0.30	57	
0.35	100	
0.40	225	
0.45	900	

With $p_1 = 0$ and $p_0 = 1/2^{k-1}$, it becomes

$$N_{\text{Yang}} > \frac{9 \cdot p_0 \cdot (1-p_0)}{(p_0 - d)^2}. \tag{24}$$

Table 1 gives some specific region sizes for various d values.

Comparing (22) and (24), it is immediate the following two results.

Result 1. The minimum size of a recognizable region between grey level g and grey level $g-1$ of the proposed scheme is the same as that between black and white region in the (k, k)-Prob.VSS scheme of the (k, n)-Prob.VSS scheme in [16].

Result 2. When our proposed scheme is applied to binary images, that is, $g = 2$, its minimum region size is the same as that in [15].

4. Converting a (k, k)-SS Scheme to a (k, n)-VSS Scheme

We now extend the above (k, k)-VSS scheme for greyscale images into a (k, n)-VSS scheme.

4.1. Construction of the Shares.

We give Example 4.1 to illustrate Algorithm 3.

Example 4.1 (continuation of Example 3.3). The greyscale (2, 3)-VSS scheme with $g = 3$. The three basic construction matrices for the three distinct (2, 2)-VSS schemes are

$$B_{i_1}^{(2,2)} = \begin{pmatrix} T\left(d^{(1)}|_w\right) \\ T\left(d^{(2)}|_w\right) \end{pmatrix}, \quad w = 1, \ldots, \binom{3}{2}. \tag{25}$$

For example, $c_{ij} = 01$, $d^{(1)} \in \{10, 00, 01, 11\}$, we let $d^{(1)}|_w = 00$, or 10, or 11. The three basis matrices are listed in Table 2 as follows.

Input: The secret image S, $S = [s_{ij}]$ in the coded form $C = [c_{ij}]$.
Output: The shadow images $D_1, \dots, D_n$.
Share construction procedure: For (k, n) scheme, we create a construction matrix with n rows from the k rows of the construction matrix of the (k, k)-VSS scheme as described previously. We do it in four steps.

Step 1: Generate $\binom{n}{k}$ distinct construction matrices for $\binom{n}{k}$ different (k, k)-VSS schemes to the same secret image. Notice that the random matrices are $R_h = X(h),\ X(h) \in \{0, \dots, \binom{n}{k} \cdot (2^{g-1} - 1)\}$. For the wth scheme, its construction matrix is

$$B_w^{(k,k)} = \begin{pmatrix} T(D^{(1)}|_w) \\ \vdots \\ T(D^{(k)}|_w) \end{pmatrix} = \begin{bmatrix} V_1^{(w)} \\ \vdots \\ V_k^{(w)} \end{bmatrix},$$ where $w = 1, \dots, \binom{n}{k},\ h = 1, 2, \dots, k$ and $D^{(h)}|_w$ is created directly from $D^{(1)}|_w, \dots, D^{(k)}|_w$
needs w group distinct random matrices, each group matrix has $k - 1$ distinct random matrices.
The $D^{(h)}|_w$ includes $k - 1$ distinct random matrices. (See Section 3.5 for details), and $V_h^{(w)}$ is a m-dimensional row vector.

Step 2: Consider a function $f : Z^+ \rightarrow Z^+,\ q \in \{1, \dots, k\},\ f(q) \in \{1, \dots, n\}$, for example, when $n = 3$ and $k = 2$, one possible such functions are $f(1) = 1,\ f(2) = 2$, or $f(2) = 1,\ f(3) = 2$, or $f(1) = 1,\ f(3) = 2$. There are $\binom{n}{k}$ different ways to define such a function. Let $w \in \{1, \dots, \binom{n}{k}\}$ and l_w be one of such functions.Here, we denote $\binom{n}{k}$ by the number of k-combinations of an n-element set.

Step 3: Generate a random matrix $\overline{B}_w^{(k,n)}$ of n rows, $\overline{B}_w^{(k,n)} = \begin{bmatrix} V_1^{(w)} \\ \vdots \\ V_n^{(w)} \end{bmatrix}$.
For $q \in \{1, \dots, k\}$, set $V_{q'}^{(w)} = V_q^{(w)}$ and $q' = f_w(q)$. In other words, substitute k rows of $\overline{B}_w^{(k,n)}$ with the rows of $B_w^{(k,k)}$ according to function f_w. For example, with $n = 3$ and $k = 2$, $\overline{B}_w^{(k,n)}$ could be $\begin{bmatrix} V_1^{(1)} \\ V_2^{(1)} \\ r \end{bmatrix}$, or $\begin{bmatrix} r \\ V_1^{(2)} \\ V_2^{(2)} \end{bmatrix}$, or $\begin{bmatrix} V_1^{(3)} \\ r \\ V_2^{(3)} \end{bmatrix}$, where r is randomly generated, $w \in \{1, 2, 3\}$

Step 4: Concatenate all $\binom{n}{k}$ different matrices $\overline{B}_w^{(k,n)}$ together and obtain $B^{(k,n)} = \overline{B}_1^{(k,n)} \circ \overline{B}_2^{(k,n)} \circ \cdots \circ \overline{B}_{\binom{n}{k}}^{(k,n)}$ as the resulting $n \times (m \cdot \binom{n}{k})$. Construction matrix for our (k, n) scheme. Finally, the hth row of $B^{(k,n)}$ is used to create share image A_h. Notice that each $\overline{B}_w^{(k,n)}$ is different from $B_w^{(k,k)}$.

Revealing: $U = D_{w_1} + D_{w_2} + \cdots + D_{w_k}$ for $w_1, \dots, w_k \in \{1, \dots, n\}$.

Algorithm 3

Table 2: Share construction procedure of $(2, 3)$-VSS scheme with $g = 3$.

	$R^{(1)}\|_w$	$d^{(1)}\|_w$	c_{ij}	$d^{(2)}\|_w = d^{(1)}\|_w \oplus \mathrm{C}$
1	00	00	01	01
2	10	10	01	11
3	11	10	01	11

We have $B_1^{(2,2)} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $B_2^{(2,2)} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $B_3^{(2,2)} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Using the $\binom{3}{2}$ possible functions f, we create 3 matrices $\overline{B}_w^{(k,n)}$ as follows:

$$\overline{B}_1^{(k,n)} = \begin{pmatrix} \overbrace{0\ 0}^{\{1,2\}} \\ 0\ 1 \\ r\ r \end{pmatrix}, \qquad \overline{B}_2^{(k,n)} = \begin{pmatrix} \overbrace{1\ 0}^{\{1,3\}} \\ r\ r \\ 1\ 1 \end{pmatrix}, \qquad \overline{B}_3^{(k,n)} = \begin{pmatrix} \overbrace{r\ r}^{\{2,3\}} \\ 1\ 1 \\ 1\ 1 \end{pmatrix}. \tag{26}$$

The first two rows of $\overline{B}_1^{(k,n)}$ are from the first two $B_1^{(2,2)}$ matrices. The first row, and the third row of $\overline{B}_2^{(k,n)}$ are from the first row and the second row of $B_2^{(2,2)}$. The second row and the third row of $\overline{B}_3^{(k,n)}$ are from the first row and the second row of $B_3^{(2,2)}$. Here, the symbol r represents a random bit, taking value 0 or 1. The two random bits in a matrix may or may not take the same value. In matrix $\overline{B}_w^{(k,n)}$, rows q_1, q_2 are copied from rows 1, 2 of matrix $B_w^{(2,2)}$, here $q_1, q_2 \in \{1, 2, 3\}$. With $\binom{3}{2}$= 3 different combinations of two elements out of the three, there are three different matrices $\overline{B}_w^{(k,n)}$. The concatenation of these $\binom{3}{2}$ matrices forms the basic matrix as below

$$\begin{aligned} B^{(k,n)} &= \begin{pmatrix} \overbrace{0\ 0}^{\{1,2\}} \\ 0\ 1 \\ r\ r \end{pmatrix} \circ \begin{pmatrix} \overbrace{1\ 0}^{\{1,3\}} \\ r\ r \\ 1\ 1 \end{pmatrix} \circ \begin{pmatrix} \overbrace{r\ r}^{\{2,3\}} \\ 1\ 1 \\ 1\ 1 \end{pmatrix} \\ &= \begin{pmatrix} \overbrace{0\ 0}^{\{1,2\}} & \overbrace{1\ 0}^{\{1,3\}} & \overbrace{r\ r}^{\{2,3\}} \\ 0\ 1 & r\ r & 1\ 1 \\ r\ r & 1\ 1 & 1\ 1 \end{pmatrix}. \end{aligned} \tag{27}$$

We now give an application of the scheme above.

Example 4.2. Application example of the greyscale (2, 3)-VSS scheme with 3 grey levels.

The secret image is shown in Figure 1(a). The three shadow images (shares) are in parts 1(b), 1(c), and 1(d). And the reconstructed image is in Figures 1(e)–1(h).

Theorem 4.3. *Algorithm 3 is a probabilistic (k, n)-VSS scheme with*

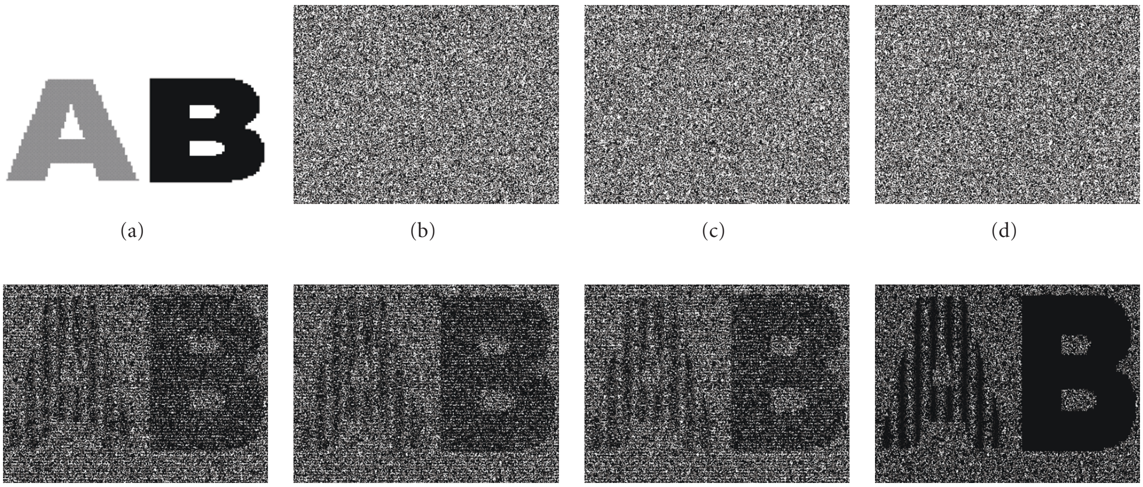
(a) (b) (c) (d) (e) (f) (g) (h)

Figure 1: (a) The secret image. (b) Share 1. (c) Share 2. (d) Share 3. (e) Share 1+Share 2. (f) Share 1 + Share 3. (g) Share 2 + Share 3. (h) Share 1 + Share 2 + Share 3.

Pixel expansion: $m_g = (g-1)\cdot\binom{n}{k}$,

Average Grey: $\beta_l = E(H(\{u_{ij} \mid s_{ij} = l\}))/m = 1 + (g - 1)(2^k - \binom{n}{k}) + (l-1)/(g-1)\cdot 2^{k-1}\cdot\binom{n}{k}$,

Average Contrast: $\alpha_l = \beta_l - \beta_{l-1} = 1/(g-1)\cdot 2^{k-1}\cdot\binom{n}{k}$.

Proof. To show security, the shares $D_1|_w, D_2|_w, \dots, D_k|_w$ are all random and all independent of each other. From the construction of the shares given in the Section 4.1, we can see that the $(k-1)\cdot\binom{n}{k}$ random matrices $D^{(1)}|_w$, $D^{(2)}|_w, \dots, D^{(k-1)}|_w$, $w = 1, \dots, \binom{n}{k}$, are all distinct and all independent of each other. Each $B_w^{(k,k)}$ forms a (k,k)-VSS scheme. We know that the k rows of matrix $\overline{B}_w^{(k,n)}$ are from the corresponding k rows of $B_w^{(k,k)}$, and can be used to reconstruct the secret image. The matrix $\overline{B}_w^{(k,n)}$ is a special (k,n)-VSS scheme, which can construct the secret image using special k rows of n rows. The matrix $B^{(k,n)}$ $(= \overline{B}_1^{(k,n)} \circ \overline{B}_2^{(k,n)} \circ \cdots \circ \overline{B}_{\binom{n}{k}}^{(k,n)})$ includes $\binom{n}{k}$ distinct submatrices, $\overline{B}_1^{(k,n)}, \overline{B}_2^{(k,n)}, \dots, \overline{B}_{\binom{n}{k}}^{(k,n)}$. In matrix $B^{(k,n)}$, there exist some special rows, which come from $B_1^{(k,k)}$, $B_2^{(k,k)}, \dots$, and $B_{\binom{n}{k}}^{(k,k)}$. From the construction method above (see in Section 4.1), those rows are distinct random rows, we cannot get any information of the secret image from the special rows of the matrix $B^{(k,n)}$. Each row of the matrix $B^{(k,n)}$ is a random matrix, namely, $A_1|_w, A_2|_w, \dots, A_k|_w$ are all random and all independent of each other. With less than k shares, no information about the secret image is revealed, thus the security of the system is ensured.

To show the pixel expansion, similar to the proposed (k,k)-VSS scheme (see Section 3), the pixel expansion $m_g = (g-1)\cdot\binom{n}{k}$ is obvious from the shadow construction process.

We now look at its Average Grey and Average Contrast.

Since $U = T(V'_{h1}) + \cdots + T(V'_{hk})$ and there is only one set V'corresponding to the (k,k)-VSS scheme. Based on Theorem 3.2 above, concatenation of random matrices does not affect the total Hamming weight. Thus

$$\begin{aligned} U_l = \left\{u_{ij} \mid s_{ij} = l\right\} &= x_U^{g-l}1^{l-1} + \left(\binom{n}{k} - 1\right)x_U^{g-1} \\ &= x_U^{[(g-1)\binom{n}{k}+1-l]}1^{l-1}. \end{aligned} \tag{28}$$

From Theorem 3.2, the Average Grey of the (k,k)-VSS scheme is $H(V')=(1-1/2^{k-1})\cdot(g-l)+(l-1)$ for the pixels with grey level l in the original image, the other $\binom{n}{k} - 1$ sets of V' are random vectors. Among these V' vectors, the number of 1's is $(1-1/2^{k-1})(g-1)$, that is

$$\begin{aligned} E(H(U_l)) &= E\left(H\left(\left\{u_{ij} \mid S_{ij} = l\right\}\right)\right) \\ &= \left(1 - \frac{1}{2^{k-1}}\right)\cdot(g-l) + (l-1) \\ &\quad + \left(\binom{n}{k} - 1\right)\left(1 - \frac{1}{2^{k-1}}\right)(g-l), \\ E(H(U_l)) &= (g-1)\cdot\binom{n}{k} + \frac{(l-1) + (1-g)\cdot\binom{n}{k}}{2^{k-1}}, \\ \beta_l &= \frac{E(H(U_l))}{m} = 1 + \frac{(l-1) + (1-g)\binom{n}{k}}{2^{k-1}\binom{n}{k}(g-1)}, \end{aligned} \tag{29}$$

Therefore, $\alpha_l = \beta_l - \beta_{l-1} = 1/(g-1)\cdot 2^{k-1}\cdot\binom{n}{k}$.

When $n = k$, Theorem 4.3 reduces to the case of the (k,k)-VSS scheme.

When $g = 2$, it reduces to a black and white VSS scheme with pixel expansion $m = \binom{n}{k}$ and Average Contrast $\alpha_l = 1/2^{k-1}\cdot\binom{n}{k}$. □

4.2. Comparison with a Previous VSS Scheme with Respect to Pixel Expansion. We will compare our scheme above with the traditional schemes in terms of their pixel expansion.

Blundo et al. [10] gave an estimate of the value of the pixel expansion of (k, n)-VSS scheme for black white image, the following Theorem 4.4 is from Lemma 3.3 of [10].

Theorem 4.4 (see [10]). *For any $n > k \geq 2$, the pixel expansion m of (k, n)-VSS scheme is*

$$m \in \left[\binom{n-1}{k-1} 2^{k-2} + 1, \left(\binom{n-1}{k-1} 2^{k-1} + 1 \right) \right]. \tag{30}$$

Muecke [11] and Blundo et al. [12] gave optimal pixel expansion m^* for in g grey level (k, n)-VSS schemes.

Theorem 4.5 (see [11, 12]). *In (k, n)-VSS scheme with g grey levels, the pixel expansion m^* and contrast α_g between grey levels are*

$$m^* = (g-1)m, \qquad \alpha_g = \frac{\alpha}{g-1}, \tag{31}$$

where m and α are pixel expansion and contrast of binary VSS schemes.

Formulas (30) and (31) imply that

$$m^* = (g-1) \cdot m \in \left[\left(\binom{n-1}{k-1} 2^{k-2} + 1 \right)(g-1), \left(\left(\binom{n-1}{k-1} 2^{k-1} + 1 \right)(g-1) \right) \right] \tag{32}$$

The relative contrast is $\alpha_i^* = 1/m^*$, $i = 0, \ldots, g-2$.

From Theorem 4.3, the pixel expansion of a probabilistic (k, n)-VSS scheme is $m_g = (g-1) \cdot \binom{n}{k}$, The Average Contrast is $\alpha_l = \beta_l - \beta_{l-1} = 1/(g-1) \cdot 2^{k-1} \cdot \binom{n}{k}$, $l = 1, \ldots, g$.

It is clear that the pixel expansion in our (k, n)-VSS scheme (see the Theorem 3.4) is smaller than that of previous deterministic (k, n)-VSS schemes [10, 11], when $k \geq n/4$, $k \geq 4$. Average contrast of our (k, n)-VSS scheme is close to that of deterministic (k, n)-VSS schemes [10, 11] when $k \geq n/2$, $k \geq 2$, and in other cases our contrast is lower than that of (k, n)-VSS schemes [10, 11].

In a deterministic SS scheme for greyscale image, we pay a higher computation complexity that the reconstruction is guaranteed. In our proposed scheme we pay smaller pixel expansion with a (small) probability of making mistake in reconstructing the secret image. In some applications we may wish a trade-off: we are willing to sacrifice some contrast in order to reduce the complexity of VSS scheme or vice versa.

4.3. The Minimum Size of Recognizable Region in (k, n)-VSS Scheme. In the proof of Theorem 4.3, we obtained:

$$\begin{aligned} U_l = \left\{ u_{ij} \mid s_{ij} = l \right\} &= x_U^{g-l} 1^{l-1} + \left(\binom{n}{k} - 1 \right) x_U^{g-1} \\ &= x_U^{[(g-1)\binom{n}{k}+1-l]} 1^{l-1}. \end{aligned} \tag{33}$$

For the pixels with grey level l in the original image, the reconstructed pixel U_l has Hamming weight $H(U_l) \in [l-1, (g-1)\binom{n}{k}]$. The probability of $H(U_l) = l - 1 + t$ is:

$$\begin{aligned} p_{l-1+t} &= \binom{(g-1)\binom{n}{k} + 1 - l}{t} \cdot \left(1 - \frac{1}{2^{k-1}} \right)^t \\ &\quad \cdot \left(\frac{1}{2^{k-1}} \right)^{[(g-1)\binom{n}{k}+1-l]-t}, \\ &\quad t = 0, \ldots, (g-1) \cdot \binom{n}{k} - l + 1. \end{aligned} \tag{34}$$

In our analysis of the region size, let random variable X_l represent the Hamming weight above, thus $X_l \in [l-1, (g-1) \cdot \binom{n}{k}]$ and X_l has a binomial distribution with mean vaue and variance:

$$\begin{aligned} \mu_x &= \left((g-1)\binom{n}{k} + 1 - l \right) \cdot \left(1 - \frac{1}{2^{k-1}} \right) + (l-1), \\ \delta_x^2 &= \left((g-1)\binom{n}{k} + 1 - l \right) \cdot \left(1 - \frac{1}{2^{k-1}} \right) \cdot \frac{1}{2^{k-1}}. \end{aligned} \tag{35}$$

Now we consider a group of N pixels with the same grey level l in the original image. Since all pixels are treated separately in the share generation, these N random variables are independent and identically distributed (i.i.d.). Therefore, the total visual effect of the region is closely related to the $Z = \sum_{i=1}^{N} X_l^{(i)}$, and

$$\begin{aligned} E(Z) &= E\left(\sum_{i=1}^{N} X_l^{(i)} \right) = \sum_{i=1}^{N} E\left(X_l^{(i)} \right) = N\mu_x \\ &= N \left[p \cdot \left((g-l) \cdot \binom{n}{k} + 1 - l \right) + (l-1) \right], \end{aligned} \tag{36}$$

where $p = 1 - 1/2^{k-1}$,

$$\begin{aligned} \mathrm{Var}(Z) &= \mathrm{Var}\left(\sum_{i=1}^{N} X_l^{(i)} \right) = \sum_{i=1}^{N} \mathrm{Var}\left(X_l^{(i)} \right) = N\sigma_x^2 \\ &= N \left[p(1-p) \left((g-l)\binom{n}{k} + 1 - l \right) \right]. \end{aligned} \tag{37}$$

Using a Gaussian distribution to approximate the above binomial distribution, we can obtain the lower bound for N. According to Empirical Rule, about 99.73% of all values fall within three standard deviations of the mean. Hence, to recognize a region of grey level l, the region size should

Table 3: Minimum region sizes of the proposed $(2, 3)$-VSS scheme with $g = 3$.

$(2, 3)$-VSS	Between grey levels 1 and 2	Between grey levels 2 and 3
with $g = 3$	$(l = 2,\ g - l = 1)$	$(l = 3,\ g - l = 0)$
$d = 0.00$	198	162
$d = 0.05$	244	200
$d = 0.10$	309	253
$d = 0.15$	404	300
$d = 0.20$	549	449
$d = 0.25$	791	646
$d = 0.30$	1235	1010
$d = 0.35$	2196	1795
$d = 0.40$	4940	4038
$d = 0.45$	19760	16150

satisfy $\mu_l - 3\sigma_l > \mu_{l-1} + 3\sigma_{l-1} + N \cdot d$, where d determines the minimum separation between the two distributions. That is

$$\begin{aligned}
&N\left[\left((g-1)\cdot\binom{n}{k}+1-l\right)p+l-1\right] \\
&\quad - 3\sqrt{N\left[\left((g-1)\binom{n}{k}+1-l\right)p(1-p)\right]} \\
&\quad > N\left[\left((g-1)\cdot\binom{n}{k}+2-l\right)p+l-2\right] \\
&\quad + 3\sqrt{N\left[\left((g-1)\cdot\binom{n}{k}+2-l\right)p(1-p)\right]} + N\cdot d \\
&\sqrt{N}(1-p-d) > 3\sqrt{p(1-p)} \\
&\quad \times \left(\sqrt{(g-1)\cdot\binom{n}{k}+1-l}+\sqrt{(g-1)\cdot\binom{n}{k}+2-l}\right) \\
&N > 9\frac{p\ (1-p)}{(1-p-d)^2} \\
&\quad \cdot \left(\sqrt{(g-1)\cdot\binom{n}{k}+1-l}+\sqrt{(g-1)\cdot\binom{n}{k}+2-l}\right)^2
\end{aligned} \tag{38}$$

where $p = 1 - 1/2^{k-1},\ (1-p-d) > 0,\ d < 1 - p = 1/2^{k-1}$.

When $k = n,\ N > 9p(1-p)\cdot(\sqrt{g-i}+\sqrt{g-l+1}/1-p-d)^2$ is the minimum region size. For a (2, 3) scheme, $n = 3$, $k = 2$, $g = 3$, when $d < 1/2^{k-1} = 0.5$, Table 3 shows the region sizes for a few d values.

5. Conclusions

This paper proposes an approach to convert a deterministic (k, k)-SS scheme to a (k, k)-VSS scheme for greyscale images with maximum number of grey levels g. Its pixel expansion factor is $g - 1$ which is independent of k and it is significantly smaller than the previous result $2^{k-1} \cdot (g - 1)$. The quality of the reconstructed image, measured in Average Contrast between consecutive grey levels, is the same as the traditional greyscale VSS schemes. When our scheme is applied to binary images, it has the same minimum size for recognizable regions as that of the Prob.VSS scheme of [15]. This (k, k)-SS scheme is extended to a more general greyscale (k, n)-VSS scheme based on XOR operations. The pixel expansion in our (k, n)-VSS scheme (see Theorem 3.4) is smaller than that of previous deterministic (k, n)-VSS schemes [10, 11], when $k \geq n/4$, $k \geq 4$. Average contrast of our (k, n)-VSS scheme is close to that of deterministic (k, n)-VSS schemes [10, 11] when $k \geq n/2$, $k \geq 2$, and in other cases our contrast is lower than that of (k, n)-VSS schemes [10, 11]. However, there remains a problem of how to ensure the favorable pixel expansion and contrast provided by (k, n)-SS scheme is also available in (k, n)- VSS scheme

Notation

Original image:	$S = \{s_{ij}\},\ i = 1, \dots, \phi,\ j = 1, \dots, \varphi,$ $s_{ij} \in \{1, \dots, g\}$
Coded image:	$C = \{C_{ij}\}, i = 1, 2, \dots, \phi,$ $j = 1, 2, \dots, \varphi, c_{ij} \in \{0, 1, \dots, g-1\}$
Reconstructed image:	$U = \{u_{ij}\}, i = 1, \dots, m \cdot \phi,$ $j = 1, \dots, m \cdot \varphi$
Number of grey levels:	g
Grey level values:	l, t
Average gray:	β_l
Average contrast:	α_l
Intermediate matrices:	$R_h = \{X_h\}, X_h \in \{0, \dots, 2^{g-1} - 1\},$ $D_h = \{d_{ij}^{(h)}\},\ h = 1, 2, \dots, n$
Shadow images:	$A_h, D_h,\ h = 1, 2, \dots, n$
Threshold value:	$k \in \{2, \dots, n\}$
A set of share indices:	$\{q_1, \dots, q_k\}$
Pixel expansion:	M
Basic matrix:	B
Binary vectors:	V
Probability:	P
Region size (pixels):	N

The number of k combinations of an n element set:	$\binom{n}{k}$
Index to (k, k) schemes in the generation of a (k, n) scheme:	$w = 1, \dots, \binom{n}{k}$
Temporary variables:	$x, y \in \{0, 1\},\ q, z \in Z^1$.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable suggestions to improve this paper. The authors thank Professor Xiaobo Li of University of Alberta for his suggestions and help in the early stage of the development of this paper. This research was supported in part by the National Natural Science Foundation of China under Grants nos. 60873249, 60902102, 60673065, 60971006, 863 Project of China under Grant 2008AA01Z419, and the Postaldoctoral Foundation of China under Grant no. 20090460316.

References

[1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the AFIPS National Computer Conference*, vol. 48, pp. 313–317, 1979.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[3] C.-C. Chang and R.-J. Hwang, "Sharing secret images using shadow codebooks," *Information Sciences*, vol. 111, no. 1–4, pp. 335–345, 1998.

[4] D. S. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognition*, vol. 40, no. 10, pp. 2776–2785, 2007.

[5] M. Naor and A. Shamir, "Visual cryptography," in *Proceedings of the Advances in Cryptology (EUROCRYPT '94)*, vol. 950 of *Lecture Notes in Computer Science*, pp. 1–12, 1994.

[6] V. Rijmen and B. Preneel, "Efficient colour visual encryption or 'Shared Colors of Benetton'," in *Proceedings of the EUROCRYPTO'96 Rump Session*, 1996, http://www.iacr.org/conferences/ec96/rump/preneel.ps.

[7] C.-N. Yang, "A note on efficient color visual encryption," *Journal of Information Science and Engineering*, vol. 18, no. 3, pp. 367–372, 2002.

[8] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, no. 7, pp. 1619–1629, 2003.

[9] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Designs, Codes, and Cryptography*, vol. 11, no. 2, pp. 179–196, 1997.

[10] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," *Designs, Codes, and Cryptography*, vol. 24, no. 3, pp. 255–278, 2001.

[11] I. Muecke, *Greyscale and colour visual cryptography*, M.S. thesis, Computer Science of Dalhousie University-Daltech, Halifax, Canada, 1999.

[12] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," *Information Processing Letters*, vol. 75, no. 6, pp. 255–259, 2000.

[13] M. Iwamoto and H. Yamamoto, "The optimal n-out-of-n visual secret sharing scheme for gray-scale images," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E85-A, no. 10, pp. 2238–2247, 2002.

[14] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E82-A, no. 10, pp. 2172–2177, 1999.

[15] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481–494, 2004.

[16] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *Computer Journal*, vol. 49, no. 1, pp. 97–107, 2006.

[17] C.-N. Yang and T.-S. Chen, "An image secret sharing scheme with the capability of previewing the secret image," in *Proceedings of the IEEE International Conference onMultimedia and Expo (ICME '07)*, pp. 1535–1538, July 2007.

[18] C.-N. Yang, A.-G. Peng, and T.-S. Chen, "Secret image sharing: DPVCS a two-in-one combination of (D)eterministic and (P)robabilistic (V)isual (C)ryptography (S)chemes," *Journal of Imaging Science and Technology*, vol. 52, no. 6, Article ID 060508, 12 pages, 2008.

[19] A. De Bonis and A. De Santis, "Randomness in secret sharing and visual cryptography schemes," *Theoretical Computer Science*, vol. 314, no. 3, pp. 351–374, 2004.

[20] S.-J. Lin and J.-C. Lin, "VCPSS: a two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches," *Pattern Recognition*, vol. 40, no. 12, pp. 3652–3666, 2007.